

INFORMATION SECURITY IN A DOWN ECONOMY

BY ERNIE HAYDEN

Tips to Protect Your Enterprise and Not Spend a Lot of Money

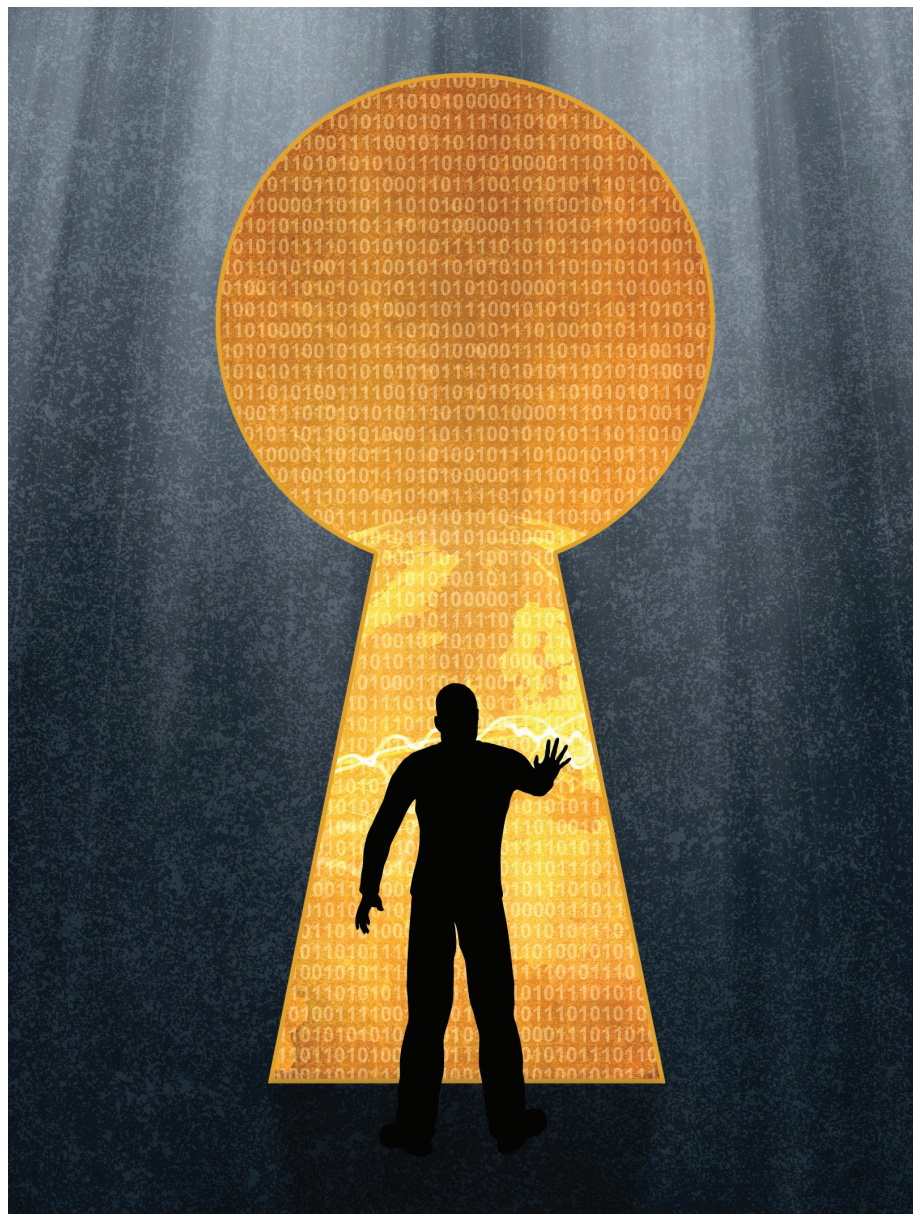
As one of my college professors said as a cliché, “It is intuitively obvious to the most casual observer...” that our economy is a mess, and the challenges posed by the Wall Street and banking crises are affecting our businesses.

Customers are not as willing to spend money, credit is not readily available, and yet we still rely on technology to protect our information, process orders and keep us in business.

Budgets are tight and the boards and managers are focused on every cost. With this environment, it certainly is hard to imagine that information security and protection of computer assets is a high priority on the minds of the corporate leadership.

Unfortunately, regulations must continue to be met such as the Payment Card Industry Data Security Standard (PCIDSS) for credit card transactions; Sarbanes Oxley audits and mandates are always present for publicly traded enterprises; and new compliance rules affecting cyber security are in play such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards that must be met by most electric utilities in North America by the end of 2009.

The bad economy is even stimulating another business – organized crime and organized cyber crime. These well-organized operations from all around the world are trying to take advantage of the economic situation by posing “get rich quick” schemes on line; tempting unemployed or underemployed workers with ways to find new jobs for a fee or even unwittingly launder money thinking they landed a great “work at home” job. And of course, the cyber-



criminals see tempting targets – those employees working in companies who can help the criminals make more money through fraud and outright theft of corporate information assets to sell on the black market.

In a word, “Whew!” As security professionals, how can we make solid arguments to our management to ensure we continue to support information security and yet not spend money on the successful achievement of this goal?

CONTINUED ON PAGE 20



In my role as a security professional at a major enterprise, I'm faced with the same challenges every day and I am often wondering how to be successful in this very difficult climate. As I think about how to proceed and talk to my peers in the industry, I tend to go towards the fundamentals. In other words what are the problems we are tasked to solve,

employees – from the receptionist to the system administrator to the manager to the Chairman of the Board. Start a process of educating your employees on what the threats are, how to avoid them, and what to do if a threat is identified. In other words, make security everyone's job.

Approaches you can consider include simple “brown bag” lunch presentations on computer security. Usually an interested employee would be glad to help do some evangelizing and get the word out to the employees. Also, you could ask your local FBI office if they'd give a talk on cybercrime and fraud. You could also approach the local chapters of InfraGard, FBI Citizens Academy Alumni Association, Information Systems Security Association (ISSA) or Information Systems Audit and Control Association (ISACA), or your Attorney General's Office for volunteer speakers to help tell stories and teach your staff that their actions – or their lack of action on the computer – could substantially protect the company.

In addition to “formal” meetings, just have some simple reminders sent out via email or in posters – remember the “Loose Lips Sink Ships?” posters – it is the same idea.

Thirty percent of all computers are still at risk from Conficker because they have not been patched.

what are the outcomes we need to achieve and how do we get there? With this in mind, here are some actionable steps an enterprise security professional can take without too much cost and still improve the firm's security.

1. Train Your Staff

The first line of security defense for any organization is comprised of all your

A final key point is to ensure your employees understand that simply “surfing” to anywhere on the Internet puts the entire company at risk. In one case this author experienced, many employees at a company were sent some exciting emails on January 2, 2009 directing them to an Asian horoscope site. The end result was numerous computers were compromised with massive “pop up” attacks – all caused by a non-business related web site.

Overall, your employees, vendors and customers can and should be encouraged to be part of your security team. They can provide excellent intelligence on suspicious activities; they can help you with information on questionable emails circulating in the company; they can definitely be part of the overall scheme of “protecting the data.”

Also, by showing respect for the employees, et al, they can also feel like you are trying to include them in the overall success of the company in these difficult times rather than treating them as disposable assets.

2. Keep Your Computers and Servers Patched and Antivirus Up to Date

What does this mean? Essentially keep your computers and servers protected from attacks and subtle infiltrations by the “bad guys” by keeping your computers up to date with security updates from the vendors.

Does this mean you need to spend \$100,000 for specialized systems and monitoring machines? Not necessarily. You can do this by taking advantage of the automated update systems offered by the vendors.

For instance, if you have Microsoft operating systems, and you can't afford the overhead of specialized update applications and software suites, why not have your servers and workstations turn on the automatic update system already built into these computer operating systems? Yes, there is a risk that an update could result in some spot problems on your computers; however, it is best to ensure your machines are up to date as quickly as possible because the “geeky miscreants” of the world are trying to take over your machines as fast as they can when they find out about a vulnerability.

A recent story making a case for this practice is the widespread Conficker/Downadup Worm that is taking advantage of those computers that were not quickly patched when the Microsoft patch was issued on October 15, 2008.

To show how bad this problem is – a problem that could have been solved by automatically patching computers on October 15, 2008, statistics have shown that the world's computers are at serious risk.

From Wikipedia: "*The New York Times* reported that Conficker had infected 9 million computers by 22 January 2009, while *The Guardian* estimated 3.5 million infected PCs. By 16 January 2009, antivirus software vendor F-Secure reported that Conficker had infected almost 9 million PCs. As of January 26 2009, Conficker had infected more than 15 million computers, making it one of the most widespread infections in recent times."¹

Even the Guardian predicted in January that about 30 percent of all computers are still at risk from Conficker because they have not been patched.²

3. Monitor Your Networks – Especially in Times of Downsizing

Sadly, these economic times are resulting in downsizing, layoffs or furloughs of your employees. As a local prosecutor in Seattle says, "Unfortunately, there may be a temptation by trained "techies" to either retaliate against the employer or simply seek their livelihood in technologically nefarious ways."

What can you do here that is not expensive but effective? First, you can recognize that you need to turn off employee computer access immediately upon – if not prior to – termination of an employee – especially someone such as a system administrator. Don't forget turning off email and remote access, too.

Secondly, after any downsizing or during any furloughs, have your staff spend some time looking for unusual data transfers, downloads, large packet emails being sent externally from the company – these could all be evidence of internally based ways to sell data.



OPSPANNER™ for An Unpredictable World

Protect your organization against costly and unnecessary losses due to an unexpected business disruption

Be Prepared ...Even In An Unpredictable World

OpsPlanner™ Software
An Easy-to-Use, Web-based, Fully Integrated Business Continuity/COOP Planning, BIA, Incident Management, and Automated Notification Tool

Business Continuity Consulting
Certified Professionals with a Proven Methodology

Contact Us For A FREE Demonstration
1-800-558-9568
www.OpsPlanner.com

PARADIGM SOLUTIONS INTERNATIONAL
In Business to Keep You in Business

4. Understand Your Risks – Focus on the Paramount Issues

Finally, in a down economy, now is the time for the enterprise executives and security professionals to best understand the risks they face and then prioritize those risks such that the limited funds available are spent on "real" and necessary risk mitigation activities.

Taking time for some thorough risk assessment reviews may be time consuming, but it usually doesn't cost as much as the high-end technology to fix one issue. Also, the risk assessments can be fairly structured and even bring together IT, risk management, compliance, and operations into the same room focused on protecting the enterprise.

Therefore, by identifying your risks, recognizing the threats that are potential attackers of your company and industry vertical, and then prioritizing your actions to address the biggest, most threatening risks, you can probably be effective in an environment of minimal fund availability.

Yes, it is a difficult time for all of us. There is uncertainty about how the Obama administration can help save the country from this difficult economic challenge which of course rolls down to how our companies and employees focus on survival. So, the conclusion of this article is to maintain the "KISS" (Keep it Simple Stupid) approach to information security by getting your employees to be part of the security team and by taking advantage of the automated systems you already have at your fingertips.

ABOUT THE AUTHOR

Ernie Hayden is an experienced information security professional in the Seattle area. He holds a Certified Information Systems Security Professional (CISSP) certification and is a Certified Ethical Hacker (CEH). He is also principal of 443 Security & Strategy Consulting (www.443consulting.com)

¹ <http://en.wikipedia.org/wiki/Conficker>

² http://www.theregister.co.uk/2009/01/19/conficker_worm_feed/